UCO BANK
Honours your Trust

Department of Information Technology

Request for Proposal (RFP) for Selection of Consultant as Qualified Security Assessor (QSA) for PCI-DSS certification in the Bank (E-tendering)

RFP Ref. No: UCO/DIT/2976/2022-23 Date: 18.03.2023

Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s)

Sl. No.	RFP Page No.	Bid Clause No.	Original bid Clause	Query sought/ Suggestions of the Bidder	Bank Response
1	44-45	1. Scoping 1.3	Asset inventory covering all the assets in scope including shared RFP Ref. No: UCO/DIT/2976/2022-23 Date: 18.03.2023 Page 45 of 111 infrastructure within detail documentation of the applications, databases, servers, desktops, laptops, network and security devices, Medias and other system components that are part of Card Data Environment (CDE).	1. Are you looking for certification of entire Card Data Environment -Issuing -Acquiring -Ecommerce – if there - Payment Gateway and any other payment channels -if applicable - Branches – if these are exposed to Card data. If so number of Branches?? Does it include any international branches? - ATMs – if included, number of ATMs - PI advise locations	Certification will be done for Bank as a whole. Bank is having around 3000 plus branches and 2500 plus ATMs/CRs.

2	47	5. Final QSA Audit & Certificatio n	Deliverables of Final QSA Audit & Certification Phase to be provided by Bidder: i. Final "Report on compliance" (ROC) for PCI DSS compliance along with "Attestation of Compliance (AOC)" and "Certificate of Compliance (COC)".	What is the target date for certification and pl confirm it will be as per PCI DSS 4.0 as latest version	Certification need to be done with latest PCI DSS version at the earliest.
3	45	Gap Assessment	Conduct on-site Gap Assessment, and report gap areas with detailed remediation actions & specific recommendations for each of non-compliance area.	Have you performed Gap assessment in the past and if so, pl advise if any sure stoppers observed, pl advise to help us work out comp controls and include efforts in pricing	This certification activity is being carried out for first time in Bank.
4	44	PART –IV: SCOPE OF THE WORK 1.2	v. High Level and Low-Level Network/Architecture Diagram vi. List of connected entities vii. List of assets (including shared infrastructure, if applicable) for: a. Internal Vulnerability Assessment and Penetration Testing b. External Network Penetration Testing c. Approved Scanning Vendor (ASV) Scan viii. List of applications (including shared infrastructure, if applicable) for: a. Internal Application Penetration Testing b. External Application Penetration Testing ix. Schedule of activities as listed in the Scope of Work along with Pre-requisite for the activities.	For the PCI DSS managed services, please advise scope Number of IPs, Device & APT Number of applications for APT Number of External IPs Number of Internal for INVA and INPT Number of Assets/Data bases for Card Data Scanning Tool Risk Assessment no of user and locations No of user Training for Implementers for PCI DSS 4.0. No Out-of-Scope VLan for segmentation penetration	Details will be shared with successful bidder.
5	18	Clause No. 3 Point 7	Appointment letters, CVs, QSA Certificate from PCI- SSC	Appointment Letters of QSAs are confidential. We'll provide every other detail, but it'll be helpful if the appointment letters are not made mandatory.	Required document need to be shared, however confidential items may be masked. However, if relevant details are masked, bank retains the right to see further information or may

					draw adverse interpretation in its discretions.
6	44	PART –IV: SCOPE OF THE WORK. Clause 1 Point i	Assets/ Locations/ Technologies/ Process/ Service Providers/ Infrastructure (including shared infrastructure) components involved in Card Holder Data (CHD) processing.	List of all services bank provides related to Credit Card/Debit Card	Details will be shared with successful bidder.
7	44	PART –IV: SCOPE OF THE WORK. Clause 1.1 Point ii	Locations, departments, and teams involved in CHD processing.	Kindly let us know the number of locations and branches to be covered under scope of work.	Certification will be done for Bank as a whole. Bank is having around 3000 plus branches and 2500 plus ATMs/CRs. Details will be shared with successful bidder.
8	44	PART –IV: SCOPE OF THE WORK. Clause 1.1 Point ii	Locations, departments, and teams involved in CHD processing.	Location of the DC and DR site.	Bank's DC & DR location is at 1 location at Bangalore and 2 location at Kolkata.
9	44	PART –IV: SCOPE OF THE WORK. Clause 1.1 Point ii	Locations, departments, and teams involved in CHD processing.	Location where servers and infrastructure are hosted. If servers are hosted at third party hosting service provider such as Amazon, then is third party hosting services PCI DSS Compliant or Certified.	Details will be shared with successful bidder.
10	44	PART –IV: SCOPE OF THE WORK. Clause 1.2 Point v.	v. IP addresses required for internal vulnerability assessment and internal penetration testing limited to the scope of audit.	No of Internal IPs in scope	Details will be shared with successful bidder.
11	44	PART –IV: SCOPE OF THE WORK.	vi. Applications required for internal application penetration testing.	No of Internal Applications in scope	Details will be shared with successful bidder.

		Clause 1.2 Point vi.			
12	44	PART –IV: SCOPE OF THE WORK. Clause 1.2 Point vii and ix.	vii. IP addresses required for external vulnerability scan by Approved Scanner Vendor (ASV) limited to the scope of audit. ix. IP addresses required for external network penetration testing.	No of External IPs in scope	Details will be shared with successful bidder.
13	44	PART –IV: SCOPE OF THE WORK. Clause 1.2 Point viii.	viii. Applications required for external application penetration testing.	No of External Applications in scope	Details will be shared with successful bidder.
14	44	PART –IV: SCOPE OF THE WORK. Clause 1.2 Point x.	x. Segments/VLANs to be considered CDE In-Scope, Non-CDE In-Scope and Out of Scope for segmentation penetration testing.	No of VLANs in scope	Details will be shared with successful bidder.
15	Page 11 of 148	CONTROL SHEET TABLE	Cost of EMD: Rs.2,00,000/- (Rupees Two Lakh Only in the form of BG)	Based on the volume of the work, may we request you to reduce the EMD value to Rs. 1,00,000/- (Rupees One Lakh Only in the form of BG)	Clause stands as per RFP
16	Page 11 of 148	CONTROL SHEET TABLE	Bidder who wishes to participate in this tender need to procure Digital Signature Certificate (for Signing and Encryption) as per Information Technology Act2000 and CVC guidelines using that they can digitally sign their electronic bids. Bidders can procure the same from any of the CCA approved certifying agencies, or they may contact M/s eProcurement Technologies Limited. at below mentioned address and they will assist them in procuring the same. Bidders who already have a valid Digital Signature	May we request to confirm if Board resolution letter having list of signing representative and self-owned digital signature will serve the signing purpose Or company name to be integrated within the Digital signature.	Encrypted digital signature should be used for uploading / submission of the documents on the e-tendering portal. For any further support regarding digital signature, please contact the helpdesk number mentioned in the RFP document.

			Certificate need not to procure the same.		
17	Page 17 of 111	3.ELIGIBILITY CRITERIA	The Bidder must have a satisfactory experience of at least 3 years of providing PCI-DSS certification services to at least two Banks out of which one should be PSU with minimum 2000 branches.	May we request to amend the clause as follows: The Bidder must have a satisfactory experience of at least 3 years of providing PCI-DSS certification services to at least one PSU/commercial private bank.	Clause stands as per RFP.
18	Page 18 of 111	3.ELIGIBILITY CRITERIA	The Bidder should have at least five PCI-DSS certified QSAs as employees on payroll.	May we request to amend the clause as follows: The Bidder should have at least three PCI-DSS certified QSAs as employees on payroll.	Clause stands as per RFP.
19	Page 44 of 111	SCOPE OF WORK 1. Scoping 1.1.2	i) Assets/ Locations/ Technologies/ Process/ Service Providers/ Infrastructure (including shared infrastructure) components involved in Card Holder Data (CHD) processing.	May we request to let us know if Bank has any asset register or centralised tool for scanning and identifying all asset involved in Card Holder Data (CHD) processing. Also let us know, which pieces of card holder data does Bank capture, store, process or transmit in their environment? Please mark your response below with Yes/No: Permanent Account Number/Credit Card Number/Debit Card Number: Loyalty Card Numbers Gift Card Numbers CVV Track 1 Data Track 2 Data Card Service Code PIN PIN Block Card Holder Name Card Expiry Date Card Holder Billing Address Card Holder Phone Numbers	Details will be shared with successful bidder.

20	Page 44 of 111		v. IP addresses required for internal vulnerability assessment and internal penetration testing limited to the scope of audit. vi. Applications required for internal application penetration testing. vii. IP addresses required for external vulnerability scan by Approved Scanner Vendor (ASV) limited to the scope of audit. viii. Applications required for external application penetration testing. ix. IP addresses required for external network penetration testing.	May we request to confirm if bidder is required to carry all these activities or they will identify the potential assets that requires these technical assessments. If bidder has to perform technical assessment, please provide a tentative number: Application number: Web: Mobile Android" iOS: API: External hosted IP address: Internal IP address:	Details will be shared with successful bidder.
21	Page 50 of 111	4. PENALTY	If any system goes down / Bank's regular work is hampered in a system due to the audit process in progress in that system, then a penalty of Rs.10,000/- will be charged for per instance / incident, subject to a maximum of 10% of the total project cost. Thereafter, the contract/purchase order may be cancelled and Performance Bank Guarantee may be revoked and also be de-empanelled.	We request you to change the clause as follows: If any system goes down / Bank's regular work is hampered in a system due to the audit process in progress in that system and reason can be attributable to the bidder, then a penalty of Rs.10,000/- will be charged for per instance / incident, subject to a maximum of 10% of the total project cost. Thereafter, the contract/purchase order may be cancelled and Performance Bank Guarantee may be revoked and also be de- empanelled.	Clause is self-explanatory
22	Page 52 of 111	6. LIQUIDATED DAMAGE	If the selected bidder fails to deliver or perform the services within the time period(s) specified in the agreement, Bank shall, without prejudice to its other remedies under the agreement, deduct from the order value,	We request to change the clause as follows: If the selected bidder fails to deliver or perform the services within the	Clause is self-explanatory

			as liquidated damages, a sum equivalent to 0.5% of the services for each week or part thereof of delay until actual delivery or performance up to a maximum deduction of 10% of the order value. Once the maximum is reached Bank may consider cancellation of the order and the Performance Security submitted may be invoked.	time period(s) specified in the agreement and delay can be attributable to the bidder, Bank shall, without prejudice to its other remedies under the agreement, deduct from the order value, as liquidated damages, a sum equivalent to 0.5% of the services for each week or part thereof of delay until actual delivery or performance up to a maximum deduction of 10% of the order value. Once the maximum is reached Bank may consider cancellation of the order and the Performance Security submitted may be invoked.	
23	Page 61 of 111	22. TERMINATION FOR CONVENIENCE	The Bank, by a written notice for a period of ninety (90) days (both in words and figures) sent to the selected Bidder/Vendor, may terminate the said Agreement/Contract, in whole or in part, at any time at its convenience. The notice of termination shall specify that the termination is for Bank's convenience, the extent to which the performance of work under the said Agreement/Contract is terminated and the date upon which such termination becomes effective.	We request to change the clause as follows: Both parties have the rights, by a written notice for a period of ninety (90) days (both in words and figures) sent to the selected Bidder/Vendor or vice- versa, may terminate the said Agreement/Contract, in whole or in part, at any time at its convenience. The notice of termination shall specify the termination reason along with date upon which such termination becomes effective.	Clause stands as per RFP
24	Page 68 of 111	33. BLACKLISTING	xii) assignment and subcontracting the Contract or any part thereof or substitution of key personnel named in the proposal without prior written approval by the Bank;	Since proposal can be submitted jointly in consortium with PCI-SSC approved ASVs, may we request to remove the clause.	Clause stands as per RFP

UCO BANK
Honours your Trust

Department of Information Technology

Request for Proposal (RFP) for Selection of Consultant as Qualified Security Assessor (QSA) for PCI-DSS certification in the Bank (E-tendering)

RFP Ref. No: UCO/DIT/2976/2022-23 Date: 18.03.2023

Corrigendum uploaded on 06.04.2023

ANNEXURE-XVIII

MASKED COMMERCIAL TEMPLATE

Table A **(in Rs.)**

Sr No.	Major activities	Total Cost of assignment (excluding GST) (a)	GST % & Amount (b)	Total cost (including GST) c=(a+b)
1	PCI-DSS Certification scoping and Gap assessment etc. as per phase 1	XXXXX	XXXXX	XXXXX
2	Handholding for gap remediation and training etc. as per phase 2	XXXXX	XXXXX	XXXXX

3	PCI-DSS Certification as per phase 3	XXXXX	XXXXX	XXXXX
4	Network VA-PT (including ASV scans) and Application VA-PT for PCI DSS Certification *ASV scans and Internal VA to be conducted quarterly as per PCI DSS	XXXXX	XXXXX	XXXXX
5	PCI-DSS recertification as per phase 4 (excl ASV Scanning)	XXXXX	XXXXX	XXXXX
	Total Cost (1+2+3+4+5) (In figures) (Cost for Year 1)	XXXXXXXX		
	Total Cost (1+2+3+4+5) (In words) **(Cost for Year 1)**	XXXXXXXX		

Table – B

Sr No.	Major activities	Total Cost of assignment (excluding GST) (a)	GST % & Amount (b)	Total cost (including GST) c=(a+b)
1	Recertification cost for Year 2	XXXXX	XXXXX	XXXXX
2	Recertification cost for Year 3	XXXXX	XXXXX	XXXXX
	Grand Total			**XXXXX**

Table-C TCO Calculation

Sl. No	Particulars	Amount including all expenses excluding GST (A)

1	**Total Cost of Table A**	**XXXXX**
2	**Total Cost of Table B**	**XXXXX**
3	**TOTAL COST OF OWNERSHIP (TCO in figures) (Sl. No. 1 + Sl. No. 2)**	**XXXXX**
4	**TOTAL COST OF OWNERSHIP (TCO in words) (Sl. No. 1 + Sl. No. 2)**	**XXXXX**

The above quotation is subject to the following considerations: -

1) Having perused the Bid Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer our services as vendor, in conformity with the said Bid Documents at rates mentioned in the commercial bid.
2) Prices quoted are inclusive of GST.
3) Applicable taxes would be deducted by the Bank at source, if any, as per prevailing rates.
4) In case of discrepancy between unit price and total price, the unit price shall prevail.
5) In case of discrepancy between figures and words, the amount in words shall prevail.
6) For the above, any decision of Bank, in this behalf shall be final, conclusive and binding on us .
7) All payments shall be made completion of the job and meeting the deliverables.
8) L1 bidder would be determined based on the Total Cost of Ownership (TCO) quoted by the bidder as per Sl. Nos. 3 & 4 of Table C given above.
9) The rate arrived shall be valid for the entire contract period.
10) No counter condition/assumption in response to commercial bid will be accepted. Bank reserves the right to reject such bid

Sign

Name of the signatory Designation

Company Seal.

Date:

Place:

ANNEXURE-XIX

COMMERCIAL TEMPLATE

Table A **(in Rs.)**

Sr No.	Major activities	Total Cost of assignment (excluding GST) (a)	GST % & Amount (b)	Total cost (including GST) c=(a+b)
1	PCI-DSS Certification scoping and Gap assessment etc. as per phase 1			
2	Handholding for gap remediation and training etc. as per phase 2			
3	PCI-DSS Certification as per phase 3			
4	Network VA-PT (including ASV scans) and Application VA-PT for PCI DSS Certification *ASV scans and Internal VA to be conducted quarterly as per PCI DSS			
5	PCI-DSS recertification as per phase 4 (excl ASV Scanning)			
	Total Cost (1+2+3+4+5) (In figures) (Cost for Year 1)			
	Total Cost (1+2+3+4+5) (In words) **(Cost for Year 1)**			

Table – B

Sr No.	Major activities	Total Cost of assignment (excluding GST) (a)	GST % & Amount (b)	Total cost (including GST) c=(a+b)
1	Recertification cost for Year 2			
2	Recertification cost for Year 3			
	Grand Total			

Table-C TCO Calculation

Sl. No	Particulars	Amount including all expenses excluding GST (A)
1	**Total Cost of Table A**	
2	**Total Cost of Table B**	
3	**TOTAL COST OF OWNERSHIP (TCO in figures) (Sl. No. 1 + Sl. No. 2)**	
4	**TOTAL COST OF OWNERSHIP (TCO in words) (Sl. No. 1 + Sl. No. 2)**	

The above quotation is subject to the following considerations: -

1) Having perused the Bid Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer our services as vendor, in conformity with the said Bid Documents at rates mentioned in the commercial bid.
2) Prices quoted are inclusive of GST.
3) Applicable taxes would be deducted by the Bank at source, if any, as per prevailing rates.
4) In case of discrepancy between unit price and total price, the unit price shall prevail.

5) In case of discrepancy between figures and words, the amount in words shall prevail.
6) For the above, any decision of Bank, in this behalf shall be final, conclusive and binding on us.
7) All payments shall be made completion of the job and meeting the deliverables.
8) L1 bidder would be determined based on the Total Cost of Ownership (TCO) quoted by the bidder as per Sl. Nos. 3 & 4 of Table C given above.
9) The rate arrived shall be valid for the entire contract period.
10) No counter condition/assumption in response to commercial bid will be accepted. Bank reserves the right to reject such bid

Sign

Name of the signatory Designation

Company Seal.

Date:

Place: